PATENT ABSTRACTS OF JAPAN

(11)Publication numb r : 2000-276329
(43)Date of publication of application : 06.10.2000

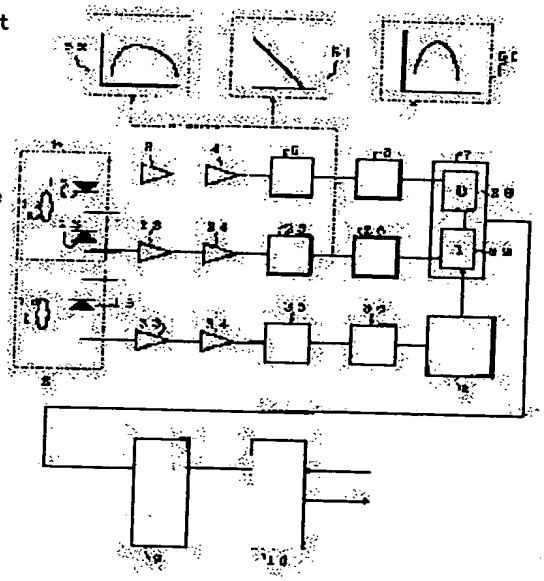
(51)Int.Cl. G06F 7/58

(21)Application number : 11-122812
(22)Date of filing : 26.03.1999

(71)Applicant : SAITO TAKESHI
(72)Inventor : SAITO TAKESHI

(54) DEVICE FOR GENERATING VERY HIGH SPEED PHYSICAL RANDOM NUMBER

(57)Abstract:
PROBLEM TO BE SOLVED: To generate true and completely uniform physical random numbers without needing random number test at all at a very high speed from 10 Mbits to 1 Gbits per sec and to inexpensively and easily utilize the generated random numbers.
SOLUTION: A random pulse signal is generated by detecting a lump of ph tons radiated from a light emitting diode(LED) 11 by avalanche (amplification type) PIN diode detectors 12, 13. One-bit random numbers are generated by setting up '0' when either one of the det ctors 12, 13 detects a lump of photons and setting up '1' when the other detector detects a lump of photons and random numbers of optional bits are generated by enumerating continuous 1-bit random numbers.



LEGAL STATUS

[Dat of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted r gistration]

[Dat of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－276329
（Ｐ2000－276329Ａ）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ

審査請求　未請求　請求項の数６　書面　（全７頁）

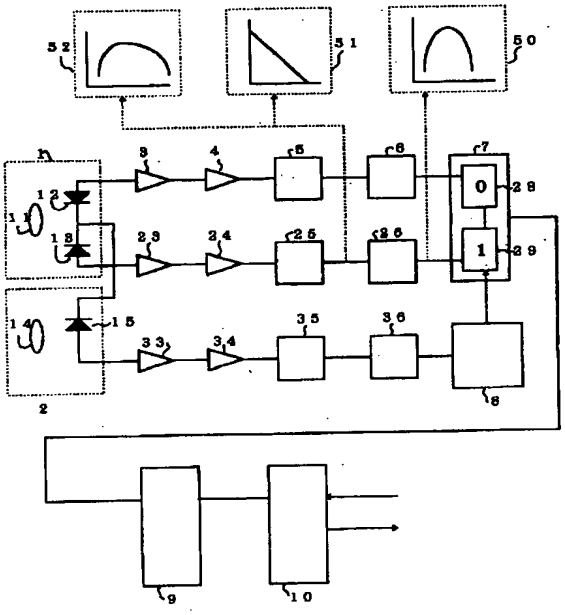
(21)出願番号　特願平11－122812

(22)出願日　平成11年３月26日(1999.3.26)

(71)出願人　597165113
斎藤　威
埼玉県入間市新光306－25
(72)発明者　斉藤　威
埼玉県入間市新光306－25

(54)【発明の名称】　超高速物理乱数生成装置

(57)【要約】
【課題】　乱数検定を全く必要としない真の完全に一様な物理乱数を、毎秒１０Ｍビットから１Ｇビットという超高速で生成させ、安価で容易に利用できるようにする。
【解決手段】　光放射ダイオード（ＬＥＤ）１１が放出する光子の塊を、アバランシェ（増幅型）ＰＩＮダイオード検出器１２、１３で検出してランダムなパルス信号を生成させる。２個の検出器１２、１３のうち一方が光子塊を検出した場合を０、もう一方が光子塊を検出した場合を１として１ビット乱数を生成し、連続するこの１ビット乱数の羅列でもって任意のビットの乱数を生成させる。



【特許請求の範囲】

【請求項１】　光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、シリコンフォトダイオードを用いて独立した各電気の塊として検出し、この各電気の塊をパルス整形器でパルスに変換して出力することにより、１秒間に１０Ｍカウント以上という速度のランダムなパルスを生成することを特徴とする超高速物理乱数生成装置。

【請求項２】　光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、１秒間に１０Ｍカウント以上というランダムパルスを生成することを特徴とする超高速物理乱数生成装置。

【請求項３】　前記２個のシリコンフォトダイオードのうち、一方のシリコンフォトダイオードが前記電気の塊を出力し、前記第１のパルス整形器で一方のパルスを出力した場合に状態が０または１となる第１記憶素子と、他方のシリコンフォトダイオードが前記電気の塊を出力し、前記第２のパルス整形器で他方のパルスを出力した場合に状態が１または０となる第２記憶素子とを設けて、これら第１記憶素子と第２記憶素子とが保持する０と１または１と０とを読み出すことにより各１ビットの乱数を生成し、この各１ビットの乱数の羅列でもって、物理乱数を生成することを特徴とする請求項２に記載の超高速物理乱数生成装置。

【請求項４】　光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、前記２個のシリコンフォトダイオードのうち、一方のシリコンフォトダイオードが前記電気の塊を出力し、前記第１のパルス整形器で一方のパルスを出力した場合に状態が０または１となる第１記憶素子と、他方のシリコンフォトダイオードが前記電気の塊を出力し、前記第２のパルス整形器で他方のパルスを出力した場合に状態が１または０となる第２記憶素子と、前記光放射ダイオードとは別に、別の光放射ダイオードからランダムに、順番に放射される光子の集団である光子塊を、別のシリコンフォトダイオードを用いて各電気の塊として検出し、この電気の塊を生成するたびに、前記１記憶素子は前記一方のパルスが出力された場合に前記０または１の状態を１または０とし、かつ、前記第２記憶素子は前記他方のパルスが出力された場合に前記１または０の状態が０または１へと切り替える切替装置とを設けて、これら第１記憶素子と第２記憶素子とが保持する０と１または１と０とを読み出すことにより各１ビットの乱数を生成し、この各１ビットの乱数の羅列でもって、物理乱数を生成することを特徴とする高速物理乱数生成装置。

【請求項５】　光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、前記２個のシリコンフォトダイオードのうち、一方のシリコンフォトダイオードが前記電気の塊を出力し、前記第１のパルス整形器で一方のパルスを出力した場合に状態が０または１となる第１記憶素子と、他方のシリコンフォトダイオードが前記電気の塊を出力し、前記第２のパルス整形器で他方のパルスを出力した場合に状態が１または０となる第２記憶素子と、前記光放射ダイオードとは別に、別の光放射ダイオードからランダムに、順番に放射される光子の集団である光子塊を、別のシリコンフォトダイオードを用いて各電気の塊として検出し、この電気の塊を生成するたびに、前記１記憶素子は前記一方のパルスが出力された場合に前記０または１の状態を１または０とし、かつ前記第２記憶素子は前記他方のパルスが出力された場合に前記１または０の状態が０または１へと切り替える切替装置とを設けて、これら第１記憶素子と第２記憶素子とが保持する０と１または１と０とを読み出すことにより各１ビットの乱数を生成し、この各１ビットの乱数の羅列でもって、物理乱数を生成する高速物理乱数生成装置を、多数基並べることにより１秒間に１Ｇビット以上という一様な物理乱数を生成することを特徴とする超高速物理乱数生成装置。

【請求項６】　前記シリコンフォトダイオードが増殖型ＰＩＮダイオードとすることを特徴とする請求項１に記載の超高速物理乱数生成装置

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、乱数生成装置に関し、ＬＥＤ（光放射ダイオード）からランダムに放出される光子の集団を、増殖型ＰＩＮダイオードでパルスとして検出して、最も完全に近い一様な真の物理乱数を、超高速で生成する物理乱数生成装置に関する。

【０００２】

【従来の技術】従来の物理乱数生成方式としては、原子核の崩壊現象というランダム現象を測定して自然乱数を生成する本願発明者による特願平９－３６３８９３９号、特願平１０－１１０１１００号などがある。しかし、これらの物理乱数生成方式では、真の自然乱数が生成できることに特徴がある。これらは乱数の生成速度が

放射線源の強度に依存しており、放射線安全管理上から１秒間に１００Ｋビットの生成速度が限界であった。

【０００３】従来のもうひとつの物理乱数生成方式として、電子回路系等のホワイトノイズを利用する方法が広く知られている。この方式は高速で乱数を生成するには適しているが、生成された乱数には、周波数に逆比例する所謂Ｆ分の１成分が含まれている。この方法ではＦ分の１成分をソフトで除去する必要があるので、厳密な意味で真の乱数とは言いがたい。

【０００４】

【発明が解決しようとする課題】従来の放射線源を利用する方法では、放射線安全管理上から１秒間に１００Ｋビットの生成速度が限界であった。ホワイトノイズを利用する方法では、Ｆ分の１成分をソフトで除去する必要があるので、厳密な意味で真の乱数は得られなかった。この発明の目的は、ＬＥＤ光源とフォトダイオード検出器という安価で安全で安定した装置により、１秒間に１Ｇビットという従来にない超高速でもって、完全に一様な真の乱数を生成させるようにする。

【０００５】

【課題を解決するための手段】第１の発明では、光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、シリコンフォトダイオードを用いて独立した各電気の塊として検出し、この各電気の塊をパルス整形器でパルスに変換して出力することにより、１秒間に１０Ｍカウント以上という速度のランダムなパルスを生成する。

【０００６】第２の発明では、光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、１秒間に１０Ｍカウント以上というランダムパルスを生成する。

【０００７】第３の発明では、光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、前記２個のシリコンフォトダイオードのうち、一方のシリコンフォトダイオードが前記電気の塊を出力し、前記第１のパルス整形器で一方のパルスを出力した場合に状態が０または１となる第１記憶素子と、他方のシリコンフォトダイオードが前記電気の塊を出力し、前記第２のパルス整形器で他方のパルスを出力した場合に状態が１または０となる第２記憶素子と、前記光放射ダイオードとは別に、別の光放射ダイオードからランダムに、順番に放射される光子の集団である光子塊を、別のシリコンフォトダイオードを用いて各電気の塊として検出し、この電気の塊を生成するたびに、前記１記憶素子は前記一方のパルスが出力された場合に前記０または１の状態を１または０とし、かつ、前記第２記憶素子は前記他方のパルスが出力された場合に前記１または０の状態が０または１へと切り替える切替装置とを設けて、これら第１記憶素子と第２記憶素子とが保持する０と１または１と０とを読み出すことにより各１ビットの乱数を生成し、この各１ビットの乱数の羅列でもって、物理乱数を生成する。

【０００８】請求項４の発明では、光放射ダイオードから、ランダムに、順番に放射される光子の集団である各光子塊を、２個のシリコンフォトダイオードを用いて択一的に各電気の塊として検出し、この各電気の一方の塊を第１のパルス整形器で一方のパルスに、他方の塊を第２のパルス整形器で他方のパルスにそれぞれ変換して互いに独立に出力することにより、前記２個のシリコンフォトダイオードのうち、一方のシリコンフォトダイオードが前記電気の塊を出力し、前記第１のパルス整形器で一方のパルスを出力した場合に状態が０または１となる第１記憶素子と、他方のシリコンフォトダイオードが前記電気の塊を出力し、前記第２のパルス整形器で他方のパルスを出力した場合に状態が１または０となる第２記憶素子と、前記光放射ダイオードとは別に、別の光放射ダイオードからランダムに、順番に放射される光子の集団である光子塊を、別のシリコンフォトダイオードを用いて各電気の塊として検出し、この電気の塊を生成するたびに、前記１記憶素子は前記一方のパルスが出力された場合に前記０または１の状態を１または０とし、かつ、前記第２記憶素子は前記他方のパルスが出力された場合に前記１または０の状態が０または１へと切り替える切替装置とを設けて、これら第１記憶素子と第２記憶素子とが保持する０と１または１と０とを読み出すことにより各１ビットの乱数を生成し、この各１ビットの乱数の羅列でもって、物理乱数を生成する高速物理乱数生成装置を、多数基並べることにより１秒間に１Ｇビット以上という一様な物理乱数を生成する。

【０００９】

【発明の実施の形態】実施の形態１．一般に、ＬＥＤ（発光ダイオード）等の光源が、１個の光子（単光子）を放射してから次に放射するまでの時間間隔をｔとすると、時間間隔ｔでもって放射される単光子の頻度分布は、以下の（１）式のように、時間間隔ｔと　時間間隔の平均値Ｔ０との比（ｔ／Ｔ０）の指数関数で表すことができる。

$$dN/dt = A\exp(-t/T0) \cdots\cdots\cdots\cdots (1)$$

ここで、平均時間Ｔ０は、１秒間に放射する光子数の平均数＜Ｎ＞の逆数でＴ０＝１／＜Ｎ＞秒である。　この

単光子は宇宙放射線観測で使用される光電子倍増管で検出することができる。

【0010】いま単光子でなく、光子の集団（光子塊）を検出する場合を考える。光子塊は複数の光子が時間的に集団を形成したもので、時間的に別の光子集団と区別できるものである。単光子はエネルギーが小さいので高価で高感度の光電子倍増管で検出するがとができ、光子塊はエネルギーが大きいので安価で比較的に感度の低いシリコン・フォト・ダイオードで検出できる。光子塊と次に放出される光子塊との間の時間間隔をｔとすると、時間間隔ｔでもって放射される光子塊の頻度分布は（１）式と同じように、時間間隔ｔと時間間隔の平均値Ｔ０との比（ｔ／Ｔ０）の指数関数で表すことができる。

$$dN/dt = A\exp(-t/T0) \cdots\cdots\cdots\cdots (2)$$

【0011】このように、単光子だけでなく、光子塊を放射する時間間隔も指数分布になるという事実及び光子塊が電気の塊、即ちパルスとして安価なシリコン・フォト・ダイオードで検出できるという実験事実が、本発明の最も重要な点である。乱数生成方式としては、時間間隔ｔを測定して１個の乱数を生成する従来の方法がある。この時間間隔を測定する方法では、時間計測における時計のクロック周波数は、コスト高とならない普通品を使用した場合１００Ｍヘルツ程度である。生成乱数の一様性はこの時計周波数に依存しており、乱数生成速度は毎秒１００Ｋビット程度が限界となる。

【0012】本発明では、２つの光検出器に０と１の状態値を択一的にそれぞれ付与し、１方の検出器に光子塊が入射した場合その出力を０、もう一方の光検出器に入射した場合その出力を１とする。光子塊の放出すなわち検出器への入射はランダムであるから、この０と１のランダムな１組を順次読み出して、１ビット乱数を生成することができる。なお、１個の光子塊は２つの光検出器のうちどちらかに択一的に入射する。

【0013】２個の検出器に０と１の状態値を択一的にそれぞれ付与して１ビット乱数を生成する本発明では、測定技術としては、光子塊検出のＯＮとＯＦＦのみで、時間測定の技術は必要ない。従って、乱数生成速度は、検出器および回路系の速度が基本となる。電子回路系の速度を、特別な技術を必要としない１０ナノ（ｎＳＥＣ）程度とすると、１ビット乱数の生成速度は毎秒１００Ｍビット程度となる。ＬＥＤ等の光源と検出器の数を並列に増やすことで、任意の乱数生成速度、例えば毎秒１Ｇビット以上の生成速度が達成できる。

【0014】２個の検出器系の感度を当初調整したとしても、ＬＥＤ、フォトダイオードや回路部品などの温度特性の違いや、波高弁別器の閾値の変動などが一定になるように保障することが重要である。従って２個の検出器とは独立（別）にもうひとつ第３の検出器系を準備して、この検出器のランダムなパルスでもって、２個の検出器に択一的にそれぞれ付与した０と１の状態値（アドレス）を逆に１と０ににそれぞれ変換する。この０と１（１と０）のアドレスを、ランダムに且頻繁に変換することにより、０と１の出現頻度を一様にし、完全に一様な１ビット乱数が生成される。

【0015】上記原理に基づく実施の形態１を以下に説明する。図１に本発明の超高速物理乱数生成装置の全体構成を示す。超高速物理乱数生成装置は、乱数生成用のランダムパルス生成素子１と、第１回路の前置増幅器３、主増幅器４、波高弁別器路５、波形整形器６と、第２回路の前置増幅器２３、主増幅器２４、波高弁別器路２５、波形整形器２６と、共通の１ビット乱数生成器７、任意ビット乱数生成器９、乱数貯蔵器１０とを備えている。更に切り替え用のランダムパルス生成素子２と前置増幅器３３、主増幅器３４、波高弁別器路３５、波形整形器３６とアドレス変換器８とを備えている。

【0016】ランダムパルス生成素子１は、乱数生成用で１個の光放射ダイオード（ＬＥＤ）光源１１および２個のアバランシェ（増殖型）ＰＴＮダイオード１２と増殖型ＰＩＮダイオード１３が一組となっている。切り替え用のランダムパルス生成素子２は、１個の光源１４と１個のＰＩＮダイオード１５が一体となっている。アドレス変換器８の出力は共通の１ビット乱数生成器７に変換駆動信号として送られる。増殖型ＰＩＮダイオード１２、１３はアバランシェ（増殖型）であり、シリコン・フォト・ダイオードの一種である。

【0017】図１では省略したが、装置全体を活性化したり光源１１を点灯する電源と装置全体を駆動する基本クロック生成回路を備えている。１ビット乱数生成器７はレジスター２８とレジスター２９とを備え、第１回路の波形整形器６の出力はレジスター２８に、第２回路の波形整形器２６の出力はレジスター２９にそれぞれ送られる。レジスター２８とレジスター２９の値は順次読み出され、任意ビット乱数生成器９に送られる。任意ビット乱数生成器９では順次受信したビット列を、４ビット又は８ビット等に区切って、乱数貯蔵器１０に送る。乱数貯蔵器１０では設定されたビット単位の乱数を格納し、必要に応じて外部の情報処理装置、計算機に転送する。

【0018】次に超高速乱数生成装置の動作を説明する。受光からパルスの生成までは、第１と第２回路とも原理が同じなので、これらをまとめて説明する。１個のＬＥＤ光源１１からの光子塊は、増殖型ＰＩＮダイオード１２または増殖型ＰＩＮダイオード１３に択一的にランダムに入射する。増殖型ＰＩＮダイオード１２、１３で生成された小電力の電気の塊は、各増殖型ＰＴＮダイオード１２、１３自体で１００倍に増殖された後、前置増幅器３、２３と主増幅器４、２４とでさらに増幅され、検出が容易な数ボルトの電圧信号となる。主増幅器

4、24からの電圧信号は波高弁別器5、25でノイズと分離され、波形整形器6、26で矩形のパルス信号となる。LED光源11からの毎秒10の7乗以上という光子塊を検出して高速パルスを生成するためには、高速でかつ信号の増倍が可能な増殖型PINダイオード12、13が必要となる。

【0019】図2は発明者による実験結果を示すグラフであり、図1のLED光源11と同特性のLED光源から放射される光子1個（単光子）を高感度の光電子増倍管でもって検出した場合の波高分布を示す。図1の第1回路で増殖型PINダイオード12、13を光電子増倍管に置き換えて、波形整形器6の出力を波高分析装置50で計測した結果である。図2のグラフでは140チャンネル当たりにピークがあり、ガウス分布となっており、LED光源からの単光子が乱数的に放射される単光子の集まりであることが分かる。

【0020】図3は、LED光源から放出された単光子の放出時間の間隔分布が指数分布であること示す実験結果である。波高弁別器路5の出力を基本クロック生成回路からの高速クロックに従って時間間隔を変化してパルスの到来数を時間カウンタ51で計測した結果である。時間間隔分布が指数分布であることは、LEDの単光子の放射がランダムな現象であることを表している。単光子がランダムな現象であれば、ランダムな単光子を集めた光子塊もまたランダムな現象となることが当然予想される。

【0021】図4は、LED光源11から放出される光子の集団（光子塊）を増幅型PINダイオード12、13で検出したときの波高分布である。波形整形器6、26の出力を波高分析装置50で計測した結果である。図4のグラフでは240チャンネル当たりにピークがあり、ガウス分布となっており、LED光源11からの光子塊が乱数的に放射される光子塊の集まりであることが分かる。同時にこの図4は、光子塊が一般的で安価なフォトダイオードを用いて充分検出できることも示している。

【0022】図5は、LED光源11から放出された光子塊の放出時間の間隔分布が指数分布であること示す実験結果である。波高弁別器路5、25の出力を基本クロック生成回路からの高速クロックに従って時間間隔を変化してパルスの到来数を時間カウンタ51で計測した結果である。図5のグラフは、LEDからの光子塊の放射時間間隔の分布が指数分布であることを示す実験結果である。図3の単光子の場合と同じように、光子塊の放射もまたランダムな現象であることを示している。即ち、増幅型PINダイオード12、13のフォトダイオードで検出した光子塊が乱数生成に利用できことを示している。

【0023】図6は、LED11から単位時間（1分間）に放射される光子塊の数の分布の実験結果であり、実曲線はガウス分布である。波高弁別器路5、25の出力を基本クロック生成回路からの高速クロックに従って時間間隔を単位時間（1分間）に固定してパルスの到来数をカウンタ52で計測した結果である。図6のグラフで放射される光子塊の数がガウス分布であることは、光子塊の放射がランダムが現象であることを示している。

【0024】光源11からのランダムな光子塊が一方のPINダイオード12に入射した場合を0（第1の波形整形器の出力パルス有りで第1レジスター28に0を設定）、他方のPINダイオード13に入射した場合を1（第2の波形整形器の出力パルス有りで第2レジスター28に0を設定）とし、1ビット乱数生成器7では、この0と1でもって各1ビット乱数を生成する。

【0025】状態変更用のランダムパルス生成素子2の光源14からの光子塊がPINダイオード15に入射した場合は、ランダムパルス生成素子1と同様に前置増幅器333、主増幅器34で増幅され、波高弁別器路35でノイズと分離され、波形整形器36で矩形のパルス信号となる。ランダムパルス生成素子2からの比較的に遅いパルス信号が生成するたびに、アドレス変換器8は、1ビット乱数生成器7のレジスター28が対応するパルス有りでそのアドレスを1に、レジスター29が対応するパルス有りでそのアドレスを0に切り替える。

【0026】この0ドレスと1ドレスとを、頻繁に且ランダムに切り替えることで、第1回路と第2回路における0と1が起こる頻度を一様にする。即ち第1回路の前置増幅器3、主増幅器4、波高弁別器路5、波形整形器6と、第2回路の前置増幅器23、主増幅器24、波高弁別器路25、波形整形器26とが品質のばらつきや時間経過による不均衡劣化により、動作性能に不均衡が生じても、この不均衡を補償して乱数を担保する。この切り替えのためのパルスは比較的に遅い1000cps（1m秒）で良いので、より安価な普通のPTNダイオード15を利用することができる。

【0027】最後に図7に、1ビット乱数生成器7からの1ビット乱数を4個並べた4ビット乱数の一様性を示す。任意ビット乱数生成器9では順次受信したビット列を、4ビットに区切って、乱数貯蔵器10に格納した。乱数貯蔵器10から読み出した外部の計算機に転送し、乱数の頻度を調べた結果である。生成乱数はほぼ完全な一様性を示している。図7に見られるわずかな一様性のばらつきは、実験上での統計的変動以内である。

【0028】光子塊の検出から1ビット乱数を生成するまでの時間は、コストを考慮して特別な回路部品や回路構成を導入しない場合、10ナノ秒程度である。従って光源11の光の強度は、毎秒10M個から100M個（cps、カウント／sec）となるように調整する。即ち1ビット乱数の生成速度は毎秒10Mから100Mビットとなる。さらに高速度で乱数生成が必要な場合は、図1のランダムパルス生成素子1等を複数個ならべ

る。例えば１００Ｍビットの１０系列のランダムパルス生成素子１等であれば、１０倍の毎秒１Ｇビットとなる。

【００２９】

【発明の効果】この発明によれば、安価で安全で安定した装置により、１秒間に１Ｇビット以上という超高速で、完全に一様な真の乱数を生成させることができる。この発明の超高速物理乱数生成装置を原子や分子の集団特性による常温超伝導のシミュレーションや多変数関数に従う世界株価の予想シミュレーションの乱数源に利用できる。

【図面の簡単な説明】

【図１】本発明の超高速物理乱数生成装置の全体の構成を示すブロック回路図である。

【図２】光電子倍増管による検出で光放射ダイオードからの単光子放射の波高分布の実験グラフである。

【図３】光電子倍増管による検出で光放射ダイオードから放射される単光子の観測時間を変化させた場合の到来頻度の実験グラフである。

【図４】シリコンフォトダイオードによる検出で光放射ダイオードからの光子塊放射の波高分布の実験グラフである。

【図５】シリコンフォトダイオードによる検出で光放射ダイオードからの光子塊の観測時間を変化させた場合の到来頻度の実験グラフである。

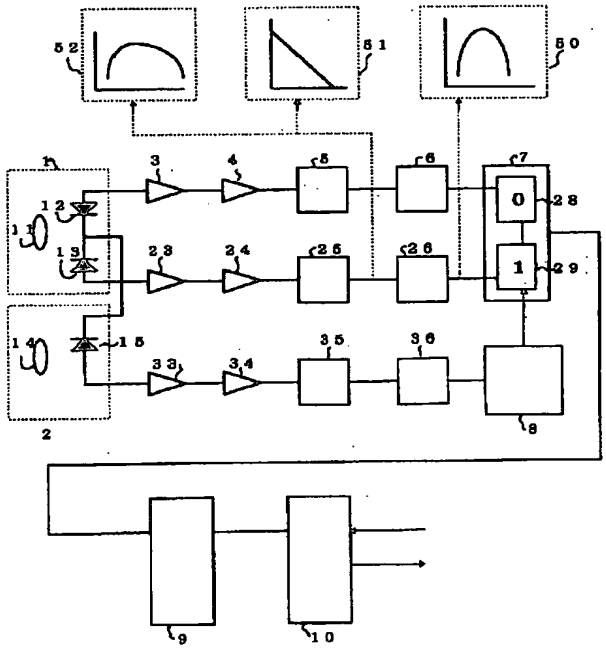
【図６】シリコンフォトダイオードによる検出で光放射ダイオードから放射される単位時間当りの光子塊数の分布がガウス分布になることを示す実験グラフである。

【図７】本発明の４列の高速物理乱数生成装置でもって生成した４ビット乱数の一様性を示す実験グラフである。

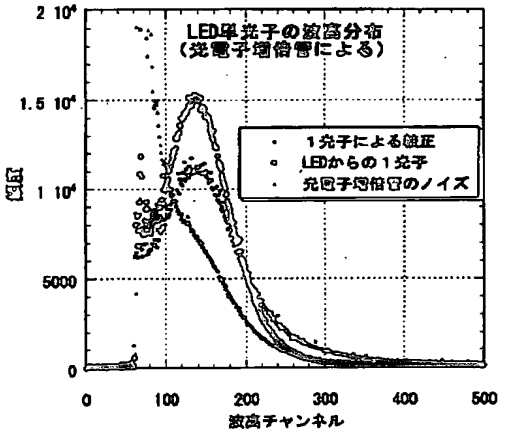
【符号の説明】

１、２　ランダムパルス生成素子
３、２３、３３　前置増幅器
４、２４、３４　主増幅器
５、２５、３５　波高弁別器
６、２６、３６　波形整形器
７　１ビット乱数生成器
８　アドレス変換器
９　任意ビット乱数生成器
１０　乱数貯臓器
１１、１４　光源（ＬＥＤ）
１２、１３　増殖型ＰＩＮダイオード検出器
１５　ＰＩＮダイオード
２８、２９　レジスター
５０　波高分析装置
５１　時間カウンタ
５２　カウンタ

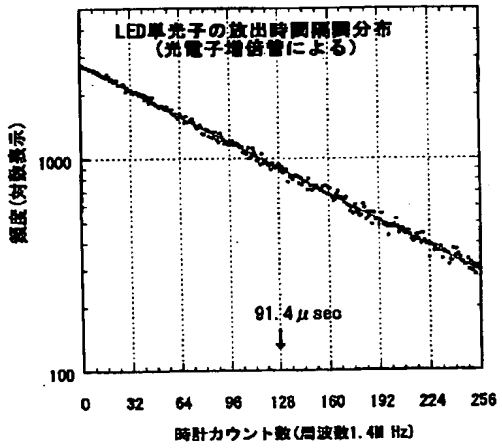
【図１】



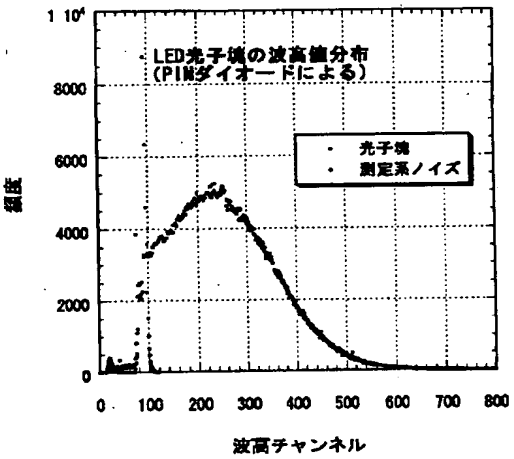
【図２】



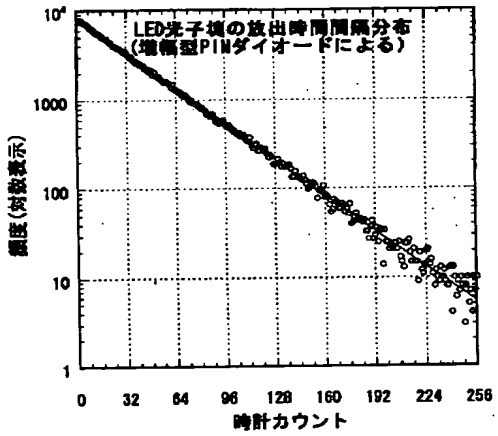
【図3】


LED単光子の放出時間間隔分布
(光電子増倍管による)
91.4μsec
頻度(対数表示)
時計カウント数(周波数1.4M Hz)

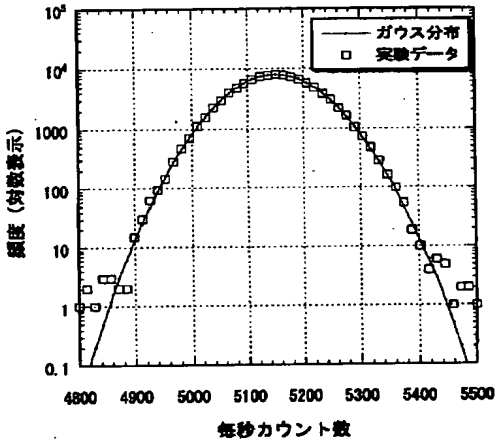
【図4】


LED光子境の波高値分布
(PINダイオードによる)
光子境
測定系ノイズ
頻度
波高チャンネル

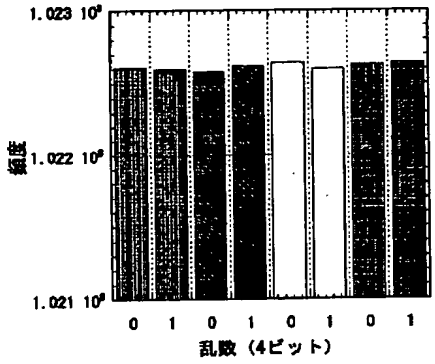
【図5】


LED光子境の放出時間間隔分布
(増幅型PINダイオードによる)
頻度(対数表示)
時計カウント

【図6】


ガウス分布
実験データ
頻度(対数表示)
毎秒カウント数

【図7】


頻度
乱数(4ビット)